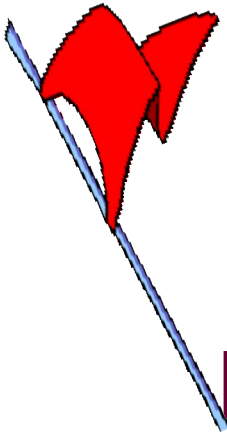
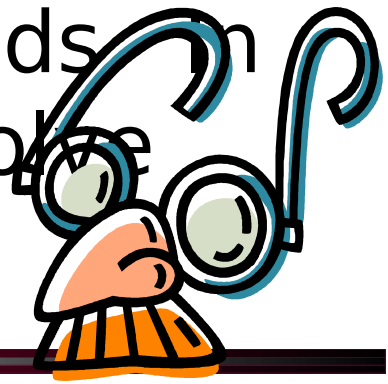


The Red Flag Rule and Medical Identity Theft Prevention Program

MEDICAL IDENTITY THEFT

"Medical Identity Theft" occurs when someone uses a person's name and other parts of their identity—such as insurance information or social security number—without the victim's knowledge or consent to obtain medical services or goods. In DOD theft may not always involve third party insurance.



Facts About Medical Identity Theft

- Fastest growing national crime
- Estimated 1 in 23 identity theft victims are victims of medical identity theft
- Nationally more than $70 to $255 billion estimated annual loss in healthcare fraud charges
- Estimated national average cost to clean up records after an incident of identity theft - $182.00 per record

Incidence of Medical Identity

Medical identity theft cases reported to Federal Trade Commission (FTC):

- 2.5 million in 2005.

- Over 3.6 million cases reported in 2007

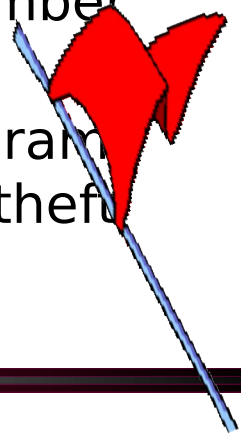
- Most are not reported.

Common Types of Medical Identity Theft

- One-off (involves relative /friend using health insurance card or the theft or selling of health insurance cards)
- Insider (employee stealing health insurance information and selling it)
- Organized Crime
- Drug-seeking Behavior

FTC Red Flags Background

- The Fair Credit Reporting Act (FCRA), enacted on October 26, 1970, is an American federal law that regulates the collection, dissemination, and use of consumer credit information and is enforced by the US Federal Trade Commission
- Fair and Accurate Credit Transactions (FACT) Act is a United States federal law, enacted on December 4, 2003, as an amendment to the FCRA
- Federal Trade Commission (FTC) Red Flags Rule – Implements sections 114 and 315 of the FACT Act, effective 1 January 2008 and enforcement is extended to 1 November 2009
- The Red Flags Rule requires each MTF to develop a program to prevent, detect, and minimize damage from identity theft



FTC Red Flags

- “Red Flags” are defined as a pattern, practice, or specific activity that indicates the possible risk of identity theft. The term “Red Flag” is used to denote the flagging/identification system to identity accounts where suspected identity theft has occurred.

- The Red Flags Rule applies to “financial institutions” and “creditors” with “covered accounts” . Medical treatment facilities (MTFs), are considered creditors since we bill some patients, extend credit to patients, allow multiple payments, or accept third-party payment for services furnished. Creditors are entities that are at risk for is identity theft.

Current Legislation and Guidance

Federal Laws

- Freedom of Information Act of 1966
- Privacy Act of 1974
- 44 USC Ch. 31 Records Management Program
- Health Insurance Portability and Accountability Act of 1996:
  - Privacy Rule
  - Security Rule
- E-Government Act of 2002
- Federal Information Security Management Act

DoD Governance

- DoD 5400.7-R DoD Freedom of Information Act Program
- DoD 5200.1-R Information Security Program
- DoD 6025.18-R DoD Health Information Privacy Regulation
- ASD(HA) Memo Breach Notification Reporting for the MHS
- DoDI 8510.01 DIACAP (C&A)
- DoD 5400.11-R DoD Privacy Program
- DoD 8580.02-R DoD Health Information Security Regulation
- DoDI 5400.16 DoD Privacy Impact Assessment (PIA) Guidance
- DoD 8500.1 & 2 Information Assurance (IA)

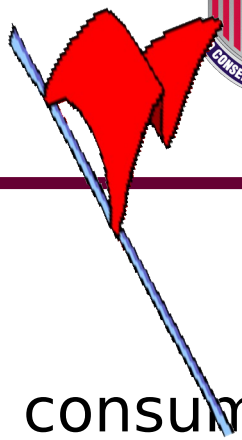
Types of Data

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)

Reporting Requirements

- Congress
- Office of Management and Budget (OMB)
- US-CERT (Computer Emergency Response Team)
- Dept of Health and Human Services (HHS)
- Assistant Secretary of Defense (Networks & Information Integration)
- DoD Inspector

Red Flag Rules



Red Flags fall into five categories:

1. Alerts, notifications, or warnings from a consumer reporting agency;
2. Suspicious documents;
3. Suspicious personally identifying information, such as a suspicious address;
4. Unusual use of – or suspicious activity relating to – a covered account; and
5. Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

FTC Red Flags Rule

- Specific FTC Red Flags Rule requirements include:
  - ***Identifying*** *relevant Red Flags and incorporate those Red Flags into the Incident Response and Reporting program*
  - ***Detecting*** *Red Flags*
  - ***Responding*** *appropriately to any Red Flags that are detected*
  - *Ensuring the program is updated and evaluated periodically*
    - *An MTF* ***Red Flag Coordinator*** *will be appointed to investigate all Red Flag inquiries*

PII/PHI Data

- The sensitivity of data is important in determining the level of protection and privacy required
- Such data may include Personally Identifiable Information (PII) and Protected Health Information (PHI)
- Even a small amount of PHI or PII can be used to determine the individual's personal identity
- The definition of data includes paper-based records as well as electronic media

Examples

Personally Identifiable Information

Information which can be used to distinguish or trace an individual's identity, including personal information which is linked or linkable to a specified individual

Protected Health Information (PHI)

Information that is created or received by a Covered Entity and relates to the past, present, or future physical or mental health of an individual; providing or payment for healthcare to an individual; and can be used to identify the individual

* Combining number of years with rank can comprise PII

Examples

- Name
- Social Security Number
- Age
- Date and place of birth
- Mother's maiden name
- Biometric records
- Marital status
- Military Rank or Civilian Grade
- Race
- Salary
- Home/office phone numbers
- Other personal information which is linked to a specific individual (including Health Information)
- Electronic mail addresses
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address
- Claim form
- Electronic claim form
- Payment history
- Account number
- Name and address of health care provider
- Diagnosis
- Number of years of military service*

Impact on the Patient

Possible Consequences of Medical Identity Theft

Wrong information in the record can lead to:

1. Future denials of insurance coverage
2. False claims that count toward a lifetime maximum
3. False diagnoses
4. Unsafe or deadly care
5. Increased insurance costs resulting from incorrect medical information.

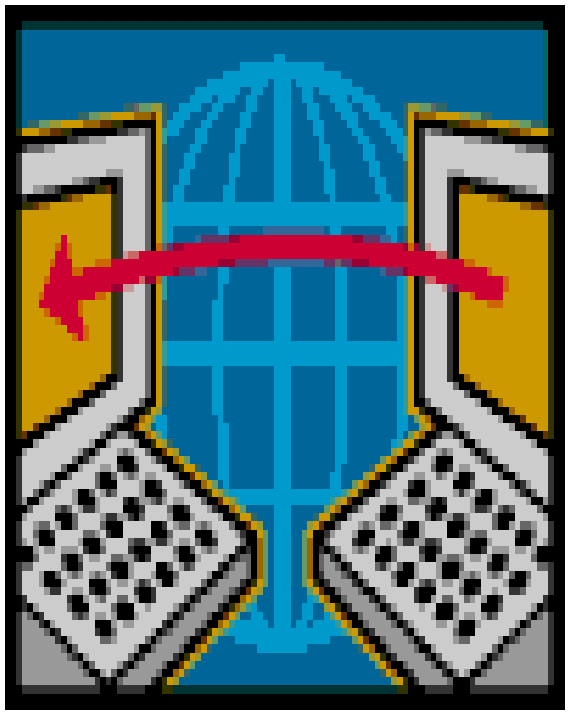
Impact on the HealthCare Provider

The provider relies on the health record for the truth of the patient's condition and status.

The ability to provide the correct treatment to the correct patient *depends* upon the accuracy of the health record.

Impact on the HealthCare Provider

When the record is on paper, separating the true from the false information can be difficult, but in the electronic record, it is even more complicated.



Impact on the HealthCare Organization

- Damaged Reputation and Lack of Trust in MTF by patients – Patients expect the information that they provide the MTF to be kept confidential and secure from theft.
- Increase costs in time and effort [illegible] in correcting erroneous informa[illegible]
- Potential lawsuits from patients
- Possible HIPAA complaint
- Possible Accreditation issues

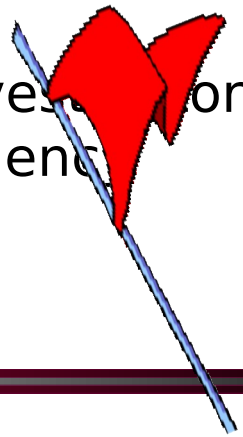
Identifying Red Flags

List of Suggested Red Flags

- A complaint or question from a patient based on the patient's receipt of:
  - A bill for another individual;
  - A bill for a product or service that the patient denies receiving;
  - A bill from a health care provider that the patient never patronized; or
  - A notice of insurance benefits (or explanation of benefits) for health care services never received.
- Records showing medical treatment that is inconsistent with an outpatient encounter, admission, or medical history as reported by the patient (Reminder, identity theft may not involve Third Party billing).
- A complaint or question from a patient about the receipt of a collection notice from a bill collector.

Identifying Red Flags List (cont'd)

- A patient or health insurer report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
- A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
- A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
- A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency.



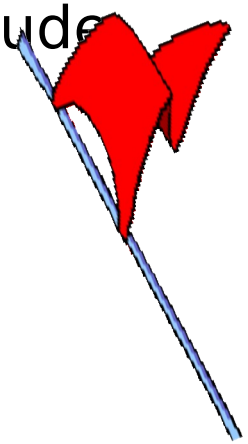
Detecting Red Flags

- Be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud
- Use patient verification processes that include Military ID photo identification. Make sure the process is as thorough as possible
- Require identifying demographic information (e.g., full name, date of birth, address, military ID, insurance card, etc.) to be verified at the time of the patient registration/check-in
- Ensure that accurate third party insurance information is collected. CHCS should be updated to reflect current information, as well as, Other Health Insurance Form (DD

Responding to Red Flags

- Promptly report the case to the immediate supervisor or Red Flag Coordinator for investigation and resolution
  - The employee should gather all documentation and report the incident to his or her immediate supervisor or the Red Flag Coordinator

- The Red Flag Coordinator will investigate and determine whether the incident is substantiated or unsubstantiated. Actions take in substantiated cases may include:
  - Cancellation of transaction;
  - Notifying appropriate law enforcement
  - Notifying the affected patient
  - Notify affected physician(s); and
  - Assess impact to practice



Best Practices to Safeguard Data and Prevent Breaches and Identity Theft

Scenario

Scenario

- You will have a a few minutes to read a scenario and decide what to do

- Be sure to think about:
  - What should you do immediately?
  - What information should be retained and why?

Scenario

- You received an e-mail asking for a copy of a patient account record and any other identifying information to be sent electronically to an insurance company for payment

- The e-mail has all the appropriate logos and identification which is linked to a well-known insurance company headquartered in Albany, New York. You sent the information as requested

- Later in the day you noticed that there were three misspelled words in the text of the e-mail. There is also an extension to the insurance company's e-mail address –"ru"- which you do not recognize

What should you do?

Scenario

- What should you do immediately?
  - Immediately notify your supervisor about these irregularities
  - Follow your breach response procedures including recording how the information was received by you
  - If appropriate, and part of your breach response process, seek assistance from Information Assurance (IA) on how to deal with this incident

Scenario

- What information should you retain and why?
  - Be sure to note down all the relevant details
  - Even if the information is not used now, it might be valuable later
  - Be prepared to describe your experience in this situation to others so that it can be used in an investigation, and as part of a group training program

Suspected ID Theft

- The FACT Act enables consumers to request and obtain a free credit report once every twelve months from each of the three nationwide consumer credit reporting companies (Equifax, Experian and TransUnion)
- You have the right to ask that nationwide consumer credit reporting companies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft
- The website, www.annualcreditreport.com, provides free access to annual credit reports
- Report suspected cases of medical identity theft to the HIPAA Privacy Officer, XXX-XXX-XXXX

Questions?
Comments?

FTC Red Flags

- “Red Flags” are defined as a pattern, practice, or specific activity that indicates the possible risk of identity theft
- “Identity Theft” occurs when someone uses a person’s name and other parts of their identity—such as insurance information or social security number—without the victim’s knowledge or consent to obtain medical services or goods, or when someone uses the person’s identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.
- The Red Flags Rule applies to “financial institutions” and “creditors” with “covered accounts” . Medical treatment facilities (MTFs), are considered creditors since we bill some patients, extend credit to patients, allow multiple payments, or accept third-party payment for services furnished. Creditors are entities that are at risk for is identity theft.